InfoCage モバイル防御
インストールガイド

InfoCage モバイル防御
Version 3.6
インストールガイド
(Windows Vista 用)

はじめに

このたびは、NEC の InfoCage モバイル防御をお買い求めいただき誠にありがとうございます。InfoCage モバイル防御は、パソコンからの情報漏洩を防止するセキュリティソフトウェアです。
ご使用になる前に本書をよくお読みになり、製品の取扱いを十分にご理解ください。

本書について

本書は、InfoCage モバイル防御を導入する手順を記載しています。InfoCage モバイル防御を導入する際にご利用ください。
また本ソフトウェアの使用に関する注意点などを記載している「2.2 注意事項」 は必ずお読みください。
セットアップが完了した後は、『InfoCage モバイル防御 ユーザーズガイド』を参照してください。

本文中の記号について

本文中では、説明、操作手順の他に以下の記号を利用しています。これらの記号の意味を正しくご理解になり、本書をお読みください。

項　目	説　　明
Notice	システムの取扱いで守らなければならない事柄や特に注意すべき点、確認すべき点を説明します。
参照	関連する内容が記載されているページを紹介しています。

用語の定義

本書では、システム操作の説明に以下のような用語を用いています。
本書を確認するにあたって前提としてご理解ください。

項　目	説　　明
InfoCage モバイル防御	パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。
暗号化	第三者の解読・利用を防ぐために、デジタル情報を組み替えることです。組み替えの際に用いられる特定の情報を「鍵」と呼びます。InfoCage モバイル防御はパソコンのドライブまたはフォルダを暗号化します。 メディア鍵認証方式では、鍵または合鍵がパソコンに装着された状態、またはネットワーク鍵にアクセスできる状態のいずれかでなければ、暗号化されたハードディスクドライブの中を閲覧することはできません。 パスワード認証方式では、ユーザパスワードを認証しない限り、暗号化されたハードディスクドライブの中を閲覧することはできません。 ただし、Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。
復号	暗号化したファイルを元に戻すことです。
セキュリティ認証	パソコンを操作可能な状態にする際に、アクセスする権利があるかどうかを確認することです。セキュリティ認証を行うと、Windows へログオンしてパソコンを操作できるようになります。これによって、パソコンの不正利用やなりすまし利用を防止します。セキュリティ認証が行われないとパソコンはロックされた状態のため、パソコン内の暗号化されたデータは読み取ることができません。
InfoCage モバイル防御ユーティリティ	InfoCage モバイル防御を使ってパソコンの保護設定を行うためのアプリケーションです。InfoCage モバイル防御をパソコンにインストールして使用します。この InfoCage モバイル防御ユーティリティを起動して、パソコンの保護設定やパスワードの変更、鍵の作成（メディア鍵認証方式）の操作を行います。
メディア鍵認証方式／パスワード認証方式	InfoCage モバイル防御の運用方式です。 インストールの際に、リムーバブルメディアを鍵としてパソコンの認証を行うメディア鍵認証方式か、またはパスワードにてパソコンの認証を行うパスワード認証方式を選択します。

項　目	説　明
スーパーバイザパスワード／ユーザパスワード	InfoCage モバイル防御ユーティリティ起動時などに必要なパスワードです。メディア鍵認証方式で運用する場合はスーパーバイザパスワードを、パスワード認証方式で運用する場合はユーザパスワードを使用します。
管理者	InfoCage モバイル防御の管理者をさします。InfoCage モバイル防御のセットアッププログラムのカスタマイズを行います。
クライアント	InfoCage モバイル防御のシステム上で管理者が管理を行うパソコンをさします。
利用者	クライアントを利用する人をさします。
保護対象	暗号化によりデータを保護するパソコンの内蔵ドライブをさします。鍵を作成する際に設定します。(メディア鍵認証方式)
メディア暗号ユーティリティ	USB メモリなどのメディアの中に暗号化したファイルを保存し、これらのファイルを InfoCage モバイル防御のインストールされていないパソコンで復号し、使用するためのユーティリティです。
外部メディア自動暗号	許可された外部メディア (許可外部メディア) へ書き出す時に自動的に暗号化を行う機能です。許可外部メディアは、同じグループ名とキーワードが設定されているパソコンでのみデータを読み書き可能で、許可されていないメディアや他のグループのパソコンではデータの読み書きはできません。
外部メディア	OS がリムーバブルメディアと認識するメディア、フロッピーディスクおよび許可外部メディアのことをさします。
許可外部メディア	外部メディア自動暗号機能によりグループ内で使用が許可されたメディア (CD-R/RW、DVD-R/+R/RW/RAM は対象外) をさします。

目 次

第1章　InfoCage モバイル防御について

InfoCage モバイル防御は、パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。
InfoCage モバイル防御では、インストール時にパソコンを使用する人を認証する「鍵」の作成、または「パスワード」の設定を行い、保護が必要なドライブまたはフォルダの暗号化を行います。
本インストールガイドに従ってそれぞれ設定を行ってください。
インストール後はパソコンを再起動する必要があります。他のプログラムを実行中の場合は、終了させてからインストールしてください。

Notice

InfoCage モバイル防御には、メディア鍵でセキュリティ認証を行う「メディア鍵認証方式」と、パスワードでセキュリティ認証を行う「パスワード認証方式」があります。
「メディア鍵認証方式」と「パスワード認証方式」の併用はできません。

1.1 InfoCage モバイル防御の特徴

InfoCage モバイル防御は、以下の機能で情報を強固に保護します。

各機能の操作方法については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

● パソコンのロック

メディア鍵認証方式の場合

鍵となるメディア等をパソコンから抜くことでパソコンをロックし、操作ができないようにします。
また、鍵をパソコンに装着することでセキュリティ認証が行われ、パソコンのロックを解除できます。

パスワード認証方式の場合

InfoCage モバイル防御のユーザパスワードが正しく入力された場合にセキュリティ認証が行われ、Windows にログオン可能になります。

※ パソコンのロック機能のみでは情報漏洩対策は万全ではありません。重要なファイルは必ず暗号化してください。

※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● **ドライブ、フォルダの暗号化**

InfoCage モバイル防御は、ドライブおよびフォルダ単位で一括して内蔵ドライブ内のデータの暗号化を行います。セキュリティ認証が行われないとパソコン内のデータは暗号化されたままのため、読み取ることができません。

メディア鍵認証方式の場合
鍵となるメディアが装着された場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。

パスワード認証方式の場合
パスワードを正しく入力した場合にセキュリティ認証が行われ、、暗号化されたファイルへアクセスが可能になります。

※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● **外部メディア自動暗号** (InfoCage モバイル防御の管理者による設定が必要)

外部メディア内のデータの暗号化を自動的に行います。所属するグループ内でのみ使用が許可される外部メディア(許可外部メディア)を設定し、この許可外部メディアへはデータは自動的に暗号化されて書き込まれ、読み込むときには自動的に復号されます。

● **メディア暗号ユーティリティ**

USB メモリなどのメディアの中に暗号化して保存したファイルを、InfoCage モバイル防御のインストールされていないパソコンで復号する場合には、メディア暗号ユーティリティを使います。

● **データの抜き取り防止** （メディア鍵認証方式のみ）

認証されていないメディアへのコピーを禁止して、情報の抜き取りを防止します。

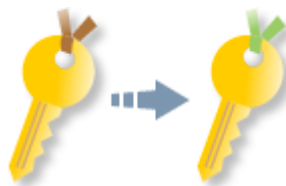
1.2 鍵とは

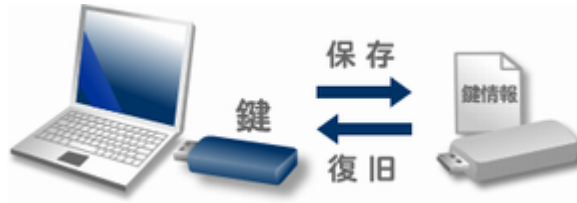
InfoCage モバイル防御で使用する鍵には以下の 2 種類があります。

● **鍵**

鍵とは、パソコンにログオンする際や暗号化されたデータにアクセスする際などに必要な認証情報をメディア等に作成したものです。
鍵がなければドアが開かないのと同様に、鍵として設定したメディアがなければ、セキュリティ認証が行われず、パソコンの情報にアクセスできません。
鍵はメディアやネットワークの共有フォルダに作成できます。

● **合鍵**

合鍵とは、スペアキーのことです。
万が一の鍵の紛失等に備えて、パソコンの保護対象ごとに一つの鍵に対して合鍵を 2 つまで作成できます。
鍵または合鍵のうちどれか 1 つで、パソコンやメディアの保護と解除ができます。

1.3 鍵情報とは

鍵のバックアップデータを鍵情報といい、鍵となるメディアとは別のメディアに保存しておきます。
鍵となるメディア内のデータを紛失した場合等は、鍵情報を元に鍵を復旧します。

> **⚠Notice**
>
> 鍵情報を紛失すると鍵の復旧ができません。鍵情報を保存したメディア内のデータを絶対に紛失しないように注意してください。

1.4 初期暗号化モード

InfoCage モバイル防御をインストールした後に実行される暗号化は、通常は「ドライブ一括暗号モード」によりドライブ単位で行われます。
ただし、InfoCage モバイル防御の管理者により「個別暗号モード」に設定されている場合は、指定したドライブおよびフォルダのみ暗号化を行います。
インストールする InfoCage モバイル防御の初期暗号化モードをあらかじめ InfoCage モバイル防御の管理者に確認してください。

● **ドライブ一括暗号モード**　（デフォルト）

● **個別暗号モード**

第2章　インストールの前にお読みください

InfoCage モバイル防御は以下の流れでインストールします。

2.1　インストールの流れ

1. セットアップ プログラムのカスタマイズ（InfoCage モバイル防御の管理者が設定）

参照 セットアッププログラムをカスタマイズする場合は、『管理者ガイド』を参照してください。

2. 利用者にセットアッププログラムを配布

3. インストール

InfoCage モバイル防御をインストールします。

参照 インストール手順は、「3.3 Step1」を参照してください。

4. 再起動

InfoCage モバイル防御のインストール後は、ログオン方法が変わります。

参照 ログオン方法は、「3.4 Windows へログオン」を参照してください。

5. 暗号化ウィザード

・パソコンの鍵および鍵情報を作成します。（メディア鍵認証方式のみ）
・フォルダ／ドライブを暗号化します。

参照 ドライブ一括暗号モードの場合 → 3.5 Step2
個別暗号モードの場合 → 第 4 章 個別暗号モードインストール

6. 終了

Notice

InfoCage モバイル防御の管理者によってセットアッププログラムがカスタマイズされた場合は、上記の手順と異なる場合があります。

2.2 注意事項

● お願い

- インストールを行う前に、「2.3 【導入前の注意事項】確認チェックシート」を使用して、インストール環境の確認を行ってください。
- 万が一に備え、大切なデータはバックアップを取ってから使用してください。

● 動作環境

- オペレーティングシステム
  以下のオペレーティングシステム（32bit 版）をサポートしています。

  Windows Vista Home Basic （日本語版）
  Windows Vista Business （日本語版）
  Windows Vista Ultimate （日本語版）

> **Notice**
> Microsoft 社から提供される最新パッチや ServicePack の適用をお奨めします。

- CPU／メモリ
  Windows Vista 各エディションの推奨システム要件に準じます。
- ハードディスクの空き容量
  本製品のインストールドライブには 45MB 以上の空き容量が必要です。
  インストールの際にはセットアップ情報を展開するために、さらに 30MB 以上の空き容量が必要です。
  また、暗号化する際には、以下の空き容量が必要です。
  必要な空き容量 ＝ 暗号化対象ファイルの中で最大のファイルと同等の容量 ＋（ドライブ容量×0.02）
  （上記は最低限必要な容量です。暗号化処理は十分な空き容量がある状態で行ってください。）
  メディア鍵認証方式の場合、初めて暗号化処理を行う場合は、保護対象に指定したドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。

● インストール前の注意事項

- InfoCage モバイル防御を Windows XP または Windows2000 で使用している場合、本バージョンへのアップグレードインストールはできません。
- InfoCage モバイル防御と共存できないアプリケーションと併用すると、正しく動作しない場合があります。インストール前に「アプリケーション競合問題について
- 」を必ず確認してください。
- インストールは、コンピュータの管理者権限を持つユーザで、日本語または英語以外の文字を含まないユーザ名で行ってください。
  InfoCage モバイル防御 ユーティリティの操作もコンピュータの管理者で行ってください。
- インストールの前にユーザアカウント制御（UAC）は有効にしてください。ユーザアカウント制御（UAC）の設定は、コントロールパネルの［ユーザアカウントの変更］より［ユーザアカウント制御の有効化または無効化］で行います。また、インストール後もユーザアカウント制御（UAC）は常に有効にしてください。
- プロダクト ID はライセンス証書に記載されています。
- NTFS ファイルシステムの暗号化、または圧縮されたファイルは InfoCage モバイル防御では暗号化できないため、NTFS ファイルシステムの暗号化、または圧縮している場合は、InfoCage モバイル防御をインストールする前に解除してください。

・ 仮想ドライブの割り当ては行わないでください。
(SUBSTコマンドおよびMOUNTVOLコマンドを使用、または「コンピュータの管理」－「ディスクの管理」でドライブ文字またはパスの変更より「次の空のNTFSフォルダにマウントする」を使用など)

● インストール後の注意事項

・ スーパーバイザパスワード／ユーザパスワードは、InfoCage モバイル防御 ユーティリティの起動時、鍵の復旧時、アンインストール時に必要になりますので、絶対に忘れないように注意してください。

・ InfoCage モバイル防御を正常にインストールした後に同じバージョンのsetup.exeを実行すると、アンインストールのウィザードが起動しますので実行しないでください。

・ InfoCage モバイル防御インストール後は ファイルシステムの変更(FATおよびFAT32からNTFSへのコンバート)は行えません。コンバートを行う場合は、一旦InfoCage モバイル防御をアンインストールしてから行ってください。

・ InfoCage モバイル防御インストール後は、OSの再インストールおよびリカバリ、または内蔵ハードディスクのフォーマットは行わないでください。これらを行う場合は、一旦InfoCage モバイル防御をアンインストールしてから行ってください。

・ Windows標準の「バックアップと復元センター」でバックアップを行う場合は、ファイルとフォルダのバックアップのみ行ってください。「Windows Complete PC バックアップ」は復元前と復元後で鍵やユーザパスワードが異なると、Windowsへのログオンやファイルの参照ができなくなりますので使用しないでください。

● 暗号化について

・ 暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。アプリケーションが使用しているファイルは、暗号化できない場合があります。

・ 暗号化や暗号化解除(復号)を行う場合、暗号化／復号処理の途中で、強制終了、Windowsのロック、スクリーンセーバの設定の変更を行うとファイルが不正になりますので、絶対に行わないでください。

・ 以下の操作を行うとデータを正しく参照できなくなりますので、絶対に行わないでください。OSにログオンできなくなった場合などでデータを退避させたい場合でも、何も操作を行わず速やかにInfoCage モバイル防御製品保守担当までご相談ください。

  * 暗号化したハードディスクを別のパソコンに接続し、データを移動する
  * セーフモードで起動し、暗号化したハードディスクから別のドライブにデータを移動する
  * Windows Vista 用の InfoCage モバイル防御 ユーティリティで暗号化したハードディスクドライブを、Windows XP/2000用のInfoCage モバイル防御をインストールしたパソコンに装着する。

・ 未割り当てのディスク領域をドライブに割り当てた場合は、再起動してから暗号化してください。再起動せずに暗号化を行うとデータが破損する可能性があります。

・ NTFSファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEMアカウントの変更権限が必要です。

参照 SYSTEMアカウントの変更方法は、「3.2.2 SYSTEMアカウントの変更方法」を参照してください。

・ NTFSファイルシステムの暗号化または圧縮されたファイルは暗号化できません。

・ 暗号化指定したフォルダを共有設定しないでください。

・ 万が一、使用中に次のような現象が発生した場合は、大切なデータを損失する可能性がありますので、現象が発生した状態のまま何も操作を行わず、速やかにInfoCage モバイル防御製品保守担当までご相談ください。

  * 暗号化したはずのファイルが読み書きできない(文字化けなど)
  * OSにログオンできない
  * 作成した鍵が使用できない(メディア鍵認証方式の場合)

● メディア鍵認証方式の注意事項

・ 事前に準備していただくもの
インストールにはリムーバブルメディアが2個必要です。
ご使用にあたっては、鍵を作成するメディア(*1)と、鍵情報を作成するためのメディア(*2)が必要です。
各メディアはインストール前にフォーマットしておいてください。

> **Notice**
> メディアをフォーマットせずに使用した場合、鍵の作成や復旧ができない場合があります。

*1:鍵は、USBメモリ、フラッシュメモリカード、モバイルディスク等の他、サーバの共有フォルダに作成できます。(推奨:USBメモリ)

*2:フロッピーディスク、USBメモリ、フラッシュメモリカード、モバイルディスク等が使用できます。

・ 注意事項

(1) 鍵について
InfoCage モバイル防御で保護されたパソコンを使用する際には、必ず鍵を作成したメディアを装着した状態で使用してください。

(2) 鍵情報について
「鍵情報」を紛失すると「鍵」の復旧ができませんので、「鍵情報」を保存したメディア内のデータを絶対に紛失しないように注意してください。

● アプリケーション競合問題について

次のアプリケーションソフトは、InfoCage モバイル防御と同時に利用、またはInfoCage モバイル防御がインストールされた環境で利用すると、問題が発生することがあります。
これらのアプリケーションソフトは InfoCage モバイル防御をインストールする前にアンインストールしておいてください。アンインストールできない場合は使用しないでください。

> **Notice**
> 下記はこれまで報告のあったアプリケーションの一覧を記載しております。記載のないアプリケーションの動作を保証するものではありません。

InfoCage モバイル防御と共存できないアプリケーション

アプリケーションの種類
・ 他のファイル暗号化ソフト、一部の独自のログオン認証を行うソフト
・ 仮想マシン環境構築ソフト(Microsoft VirtualPC など)
・ データバックアップ、リカバリソフト (PowerX StandbyDisk4、FINALDATA2007、Acronis True Image LE、Acronis True Image 10 など)
・ 一部の PC プレインストールソフト (IBM/レノボ製 PC に付属のバックアップソフト「Rapid Restore Ultra/Rescue and Recovery」 など)
・ Windows ReadyBoost
・ Windows ミーティング スペース
・ BitLocker

2.3 【導入前の注意事項】確認チェックシート

InfoCage モバイル防御をインストールする前に、以下の項目をチェックしてください。

	確 認 事 項	チェック欄	
		メディア鍵 認証方式	パスワード 認証方式
1	重要なデータは、念のためバックアップを取ること。		
2	鍵用のメディア、あるいはサーバを用意すること。		
3	十分な空き容量が各ドライブにあること。 ※暗号化を実行する際、テンポラリ(一時作業スペース)として以下の空き容量がドライブ毎に必要になります。 必要な空き容量 ＝ 暗号化対象ファイルの中で最大のファイルと同等の容量 ＋ (ドライブ容量×0.02) (上記は最低限必要な容量です。暗号化処理は、十分な空き容量がある状態で行ってください。) ※ただし、初めて暗号化処理を行う場合はすべてのドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。		
4	共存不可のアプリケーションの確認・対策を行うこと。 ※「アプリケーション競合問題について 」を参照		
5	暗号化するフォルダやファイルに SYSTEM アカウントの変更権限があることを確認すること。		
6	デュアルブートマシンでないこと。		
7	仮想ドライブを割り当てていないこと。		

第3章 インストール

InfoCage モバイル防御のインストールを行います。

3.1 インストールの前に

■ 確認事項

インストールの前に次のことを確認してください。

□ 注意事項はすべて確認しましたか？

注意事項は「2.2 注意事項」を参照してください。

□ 「【導入前の注意事項】確認チェックシート」を実施しましたか？

確認チェックシートは「2.3 【導入前の注意事項】確認チェックシート」を参照してください。

□必要なものは揃っていますか？

InfoCage モバイル防御の管理者から次のものが配布または通知されているか確認してください。

	運用方法の通知（メディア鍵認証方式またはパスワード認証方式） ※
	プロダクト ID の通知
	鍵および鍵情報を保存するメディアの配布 （メディア鍵認証方式の場合）
	暗号化するドライブ／フォルダの通知 （個別暗号モードインストールの場合） ※
	許可外部メディアの配布 （許可外部メディアを利用する場合）

（※） InfoCage モバイル防御の管理者より、あらかじめセットアッププログラムに設定されている場合があります。

3.2　パソコンの環境チェック

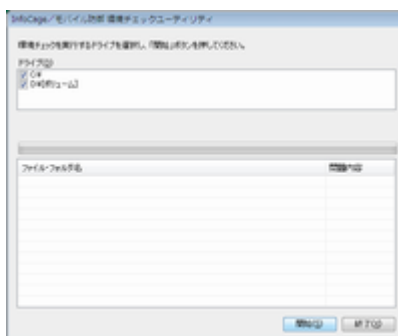
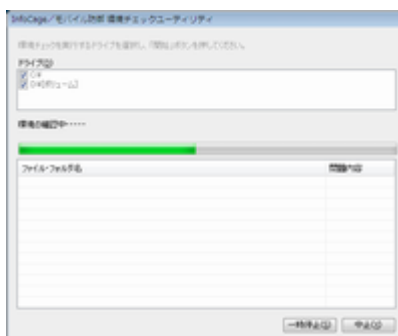
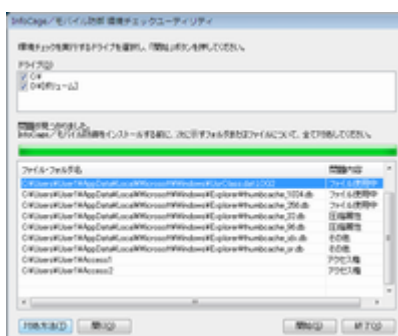
インストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境をチェックしてください。

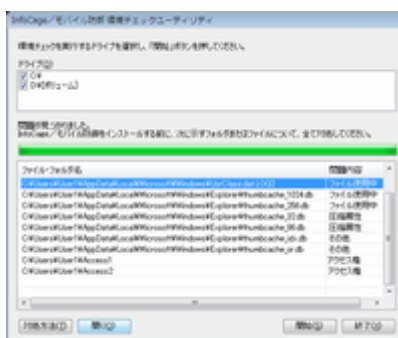
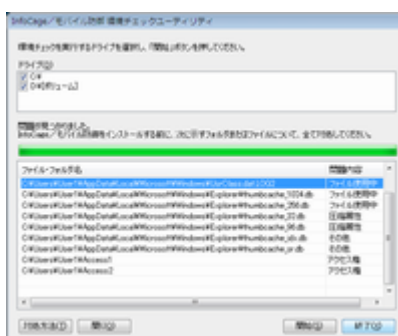
3.2.1　環境チェックユーティリティ

1. InfoCage モバイル防御が格納されているメディア (例 CD-ROM) 内の¥Vista¥Tools¥環境チェック UTL ¥MPEnvChk.EXE を実行してください。

> **Notice**
> CD-ROM からコピーして使用する場合は、環境チェック UTL フォルダをデスクトップなどにコピーしてから実行してください。(MPEnvChk.EXE は実行ファイルのみをコピーしても動作しません。)

2. 環境チェックユーティリティの説明が表示されます。
「OK」をクリックして、起動しているアプリケーションや常駐プログラムを必ず終了してください。

3. 「ドライブ」に表示されているドライブのうち、暗号化するドライブにチェックを入れ、「開始」をクリックしてください。

4. 環境をチェックしています。しばらくお待ちください。

5. 問題が見つかった場合は、「ファイル･フォルダ名」に表示されているファイルを選択し、「対処方法」をクリックします。

6. 対処方法が表示されます。内容を確認し、「閉じる」をクリックします。

7. ファイルを選択している状態で「開く」をクリックすると、ファイルのあるフォルダが開きます。
対処方法に表示されていた内容に従って、対処してください。

8. 環境チェックユーティリティを終了する場合は、「終了」をクリックします。

9. 問題の一覧を保存する場合は「はい」をクリックします。

10. 保存する場所を指定し、「保存」をクリックします。

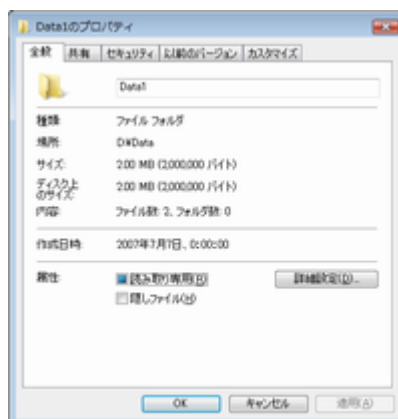
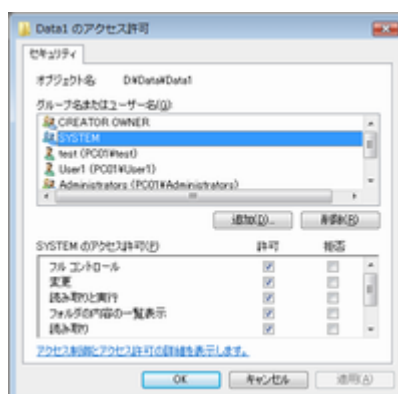
11. ファイルに出力しました。「OK」をクリックします。

以上で環境チェックは完了です。

見つかった問題の対処が完了したら、InfoCage　モバイル防御をインストールします。

3.2.2 SYSTEM アカウントの変更方法

NTFS ファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEM アカウントのフルコントロール権限または変更権限が必要です。
ここでは D:¥Data¥Data1 フォルダの SYSTEM アカウントを変更する方法を説明します。

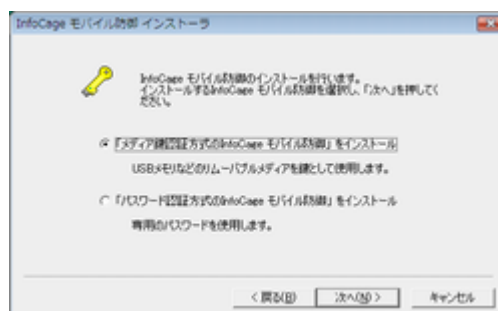
1. SYSTEM アカウントを変更したいフォルダを右クリックし、表示されるメニューの中から「プロパティ」をクリックしてください。フォルダのプロパティ画面が表示されます。

2. 「セキュリティ」タブを選択し、「編集」をクリックしてください。アクセス許可の編集画面が表示されます。
「グループ名またはユーザ名」から「SYSTEM」を選択し、「アクセス許可」の「フルコントロール」の「許可」にチェックを入れ、「OK」をクリックしてください。
これで SYSTEM アカウントが変更されました。「OK」をクリックして画面を閉じます。

Notice

「グループ名またはユーザ名」内に「SYSTEM」が表示されていない場合は、次の方法で表示させてください。
1. 「グループ名またはユーザ名」の下の「編集」をクリックし、「アクセス許可」の画面で「追加」をクリックします。
2. 表示された画面の「選択するオブジェクト名を入力してください」に「SYSTEM」と入力し、「名前の確認」をクリックします。
3. 「選択するオブジェクト名を入力してください」に「SYSTEM」と表示されますので、「OK」をクリックします。

3.3　Step1

InfoCage モバイル防御をインストールします。下記の手順で操作してください。

1. InfoCage モバイル防御が格納されているメディア（例 CD-ROM）内の setup.exe を実行し、「次へ」をクリックしてください。

2. 『「メディア鍵認証方式の InfoCage モバイル防御」をインストール』または『「パスワード認証方式の InfoCage モバイル防御」をインストール』のいずれかを選択し、「次へ」をクリックしてください。

⚠Notice

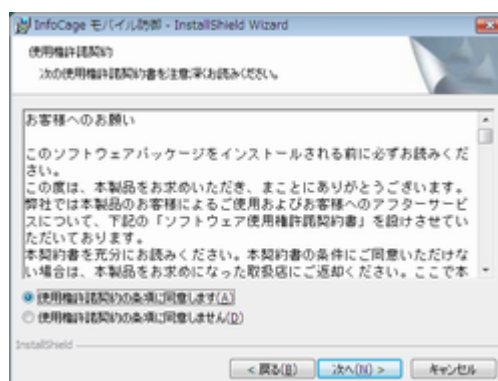
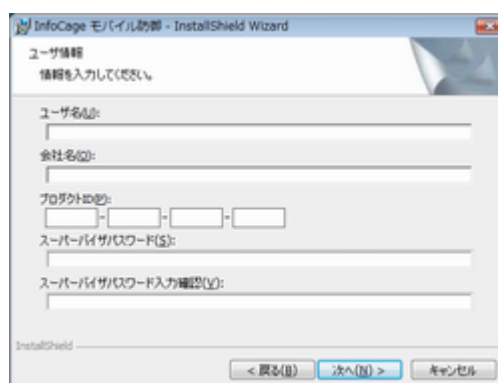
InfoCage モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。

3. 「導入前の注意事項」 画面が表示されます。
各項目をクリックすると詳細な説明が表示されますので、必ずすべての注意事項を確認し、チェックを付けてください。
すべての確認が終わりましたら、「閉じる」をクリックしてください。

> **⚠ Notice**
> 画面はメディア鍵認証方式のものです。パスワード認証方式の場合は一部異なります。

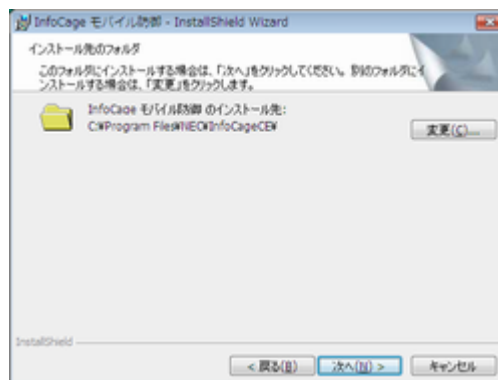
4. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。
インストールを続ける場合は「はい」を、インストールを中止する場合は「いいえ」を、*1* の画面に戻る場合は「キャンセル」をクリックしてください。

5. 「次へ」をクリックしてください。

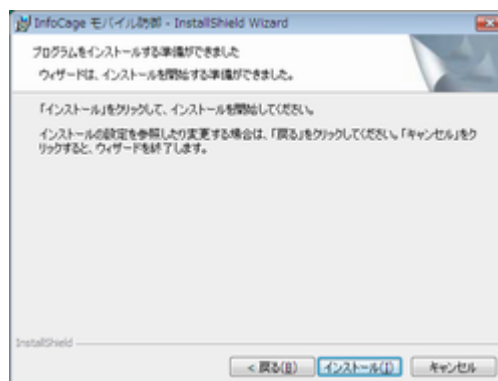
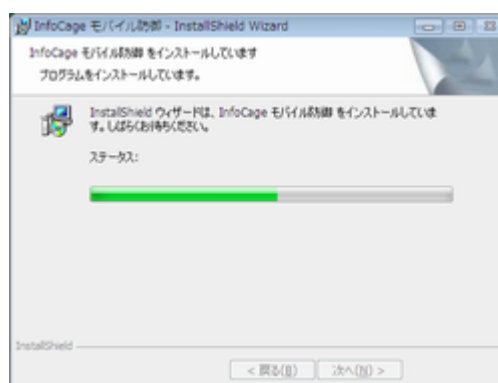
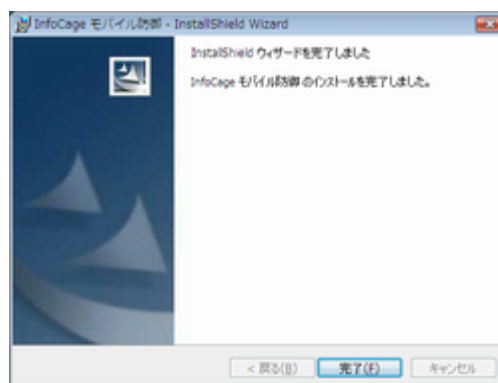
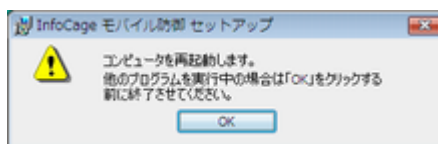
6. 使用権許諾契約をすべて確認し、同意する場合は「使用権許諾の条項に同意します」をクリックしてください。
「使用権許諾の条項に同意しません」を選択した場合はインストールできません。

7. ユーザ情報を入力します。
ユーザ名、会社名、プロダクトID、スーパーバイザパスワード／ユーザパスワードを入力します。
（確認のため、スーパーバイザパスワード／ユーザパスワードは２回入力してください。）
すべての入力が終わりましたら、「次へ」をクリックしてください。

ユーザ名、会社名	半角 40 文字以内、または全角 20 文字以内で入力してください。
プロダクトID	ライセンス証書に記載されているものを半角文字で入力してください。（大文字小文字は区別しません）。
スーパーバイザパスワード	8 文字以上 64 文字以内の半角英数および記号を指定してください。（大文字小文字を区別します）。
ユーザパスワード	8 文字以上 32 文字以内の半角英数および記号を指定してください。（大文字小文字を区別します）

⚠Notice

- 画面はメディア鍵認証方式版のものです。パスワード認証方式版の場合は、「スーパーバイザパスワード」の欄は「ユーザパスワード」と表示されます。
- スーパーバイザパスワード／ユーザパスワードとは InfoCage モバイル防御ユーティリティを起動するときなどに必要なパスワードです。忘れないよう注意してください。

8. インストール先のフォルダ選択画面で InfoCage モバイル防御のインストールフォルダを選択します。
通常はそのまま「次へ」をクリックしてください。

Notice

日本語または英語以外の文字を含むフォルダにインストールすることはできません。

9. 「インストール」をクリックしてインストールを開始してください。

10. インストール中です。しばらくお待ちください。

11. インストールが完了すると下記の画面が表示されます。
「完了」をクリックしてください。

12. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。
他のプログラムを実行中の場合は、終了させてください。
「OK」をクリックすると、パソコンが再起動します。

再起動後の操作は、次章以降を参照してください。

3.4 Windows へログオン

InfoCage モバイル防御をインストールすると、Windows のログオン方法が変わります。
以下を行うことでセキュリティ認証を行い、Windows へログオンしてパソコンを操作できるようになります。

- **メディア鍵認証方式の場合**

  鍵となるメディア等をパソコンに装着することでセキュリティ認証を行います。
  （鍵となるメディア等は、鍵の作成の完了後に装着が必要となります。
  InfoCage モバイル防御のインストール後に初めて Windows にログオンする際は、通常のログオンとなります。）

- **パスワード認証方式の場合**

  InfoCage モバイル防御のユーザパスワードを入力することでセキュリティ認証を行います。

以下の手順で Windows へログオンします。
（画面は Windows Vista Ultimate のものです。）

1. InfoCage モバイル防御のボタンをクリックします。

2. Windows のユーザ名およびパスワードを入力し、 をクリックするか Enter キーを押すと、Windows へログオンすることができます。
   パスワード認証方式の場合は「InfoCage/モバイル防御 パスワード」に、インストール時に設定したユーザパスワードを入力してください。

Notice

画面はメディア鍵認証方式のものです。

●ユーザ情報エラーの場合

メディア鍵認証方式の場合は鍵を抜いた状態、パスワード認証方式の場合は誤ったユーザパスワードでログオンしようとすると、「Windows のユーザ情報、または InfoCage モバイル防御の認証情報が違います。」 と表示され、Windows へログオンできません。
「OK」をクリックして、*2* に戻って操作してください。

続いて本ガイドの「3.5 Step2」へ進み、それぞれの認証方式の項を参照してください。

3.5.1　メディア鍵認証方式の場合

3.5.2　パスワード認証方式の場合

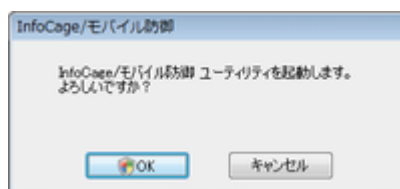
InfoCage モバイル防御の管理者の設定により、個別暗号モードでインストールした場合は、「第 4 章 個別暗号モードインストール」へ進んでください。

3.5　Step2

再起動後、暗号化ウィザードが起動します。
それぞれの認証方式の説明にしたがって、暗号化を行ってください。

> ⚠ *Notice*
>
> 何らかの理由で暗号化ウィザードを終了した場合、再度暗号化ウィザードを起動するには、スタートメニューから［すべてのプログラム］－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーティリティ］をクリックします。

3.5.1　メディア鍵認証方式の場合

1. 再起動後に、以下の画面が表示されます。「OK」をクリックしてください。

> ⚠ *Notice*
>
> 「キャンセル」をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザードを起動して、パソコンの鍵を作成および暗号化を行ってください。

2. 鍵を格納するメディアと鍵情報を格納するメディアを装着し、インストール時に設定したスーパーバイザパスワードを入力して「次へ」をクリックしてください。

3. 鍵および鍵情報を作成します。
鍵を格納するメディア　および　鍵情報を格納するメディアのドライブを選択してください。
格納するメディアが表示されないときは、「更新」をクリックします。
「次へ」をクリックしてください。

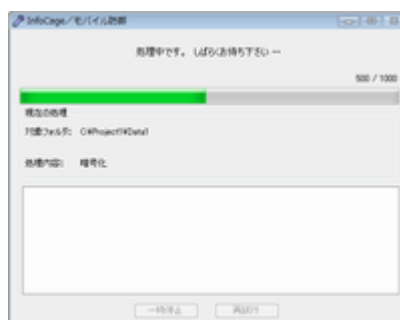
⚠ Notice

- InfoCage　モバイル防御の管理者によりあらかじめ鍵および鍵情報の格納先が設定されている場合は上記の画面が異なります。
- ここではネットワークの共有フォルダに鍵を作成することはできません。共有フォルダに鍵を作成する場合は一旦リムーバブルメディアに鍵を作成し、暗号化終了後に合鍵として作成してください。

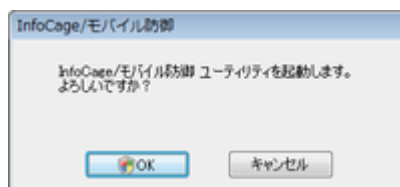
4. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。
「はい」をクリックすると暗号化が開始されます。

⚠ Notice

アプリケーションが使用しているファイルは、暗号化できない場合があります。
暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお勧めします。

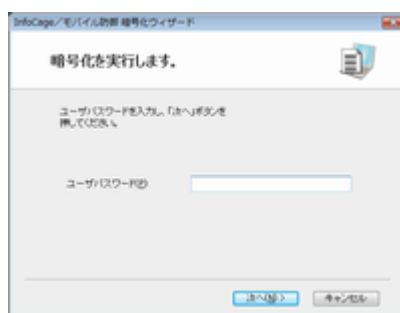
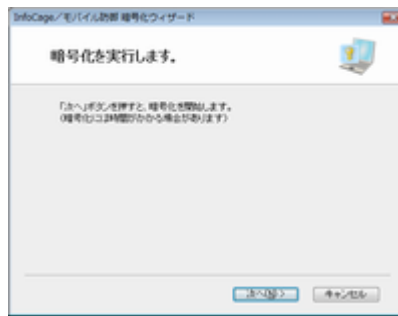
5. 暗号化処理中です。しばらくお待ちください。

6. 暗号化を完了しました。
「完了」をクリックしてください。

以上で暗号化は完了しました。
その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

3.5.2 パスワード認証方式の場合

1. 再起動後に、以下の画面が表示されます。「OK」をクリックしてください。

Notice

「キャンセル」をクリックすると、本プログラムが終了します。その場合は、後で必ずスタートメニューから[すべてのプログラム]－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーティリティ]をクリックし、暗号化を行ってください。

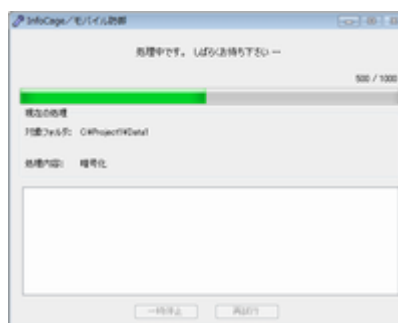
2. ユーザパスワードを入力して「次へ」をクリックしてください。

3. 暗号化を実行します。「次へ」をクリックしてください。

Notice

暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

4. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。
「はい」をクリックすると暗号化が開始されます。

Notice

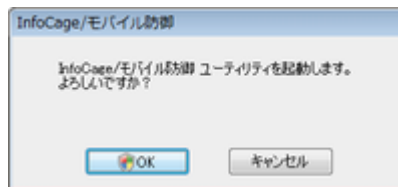
アプリケーションが使用しているファイルは、暗号化できない場合があります。
暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお勧めします。

5. 暗号化処理中です。しばらくお待ちください。

6. 暗号化を完了しました。
「完了」をクリックしてください。

以上で暗号化は完了しました。
その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

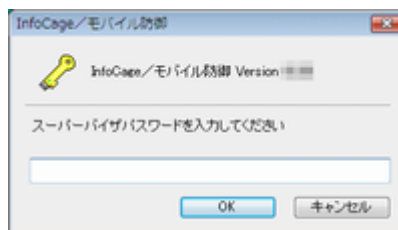
第4章　個別暗号モードインストール

InfoCage モバイル防御は、インストール後の暗号化モード（ドライブ一括暗号モード または 個別暗号モード）を InfoCage モバイル防御の管理者により設定することができます。
「個別暗号モード」に設定されたセットアップブログラムを使用した場合、インストールを完了し再起動した後は、本章のそれぞれの認証方式の説明にしたがって操作してください。

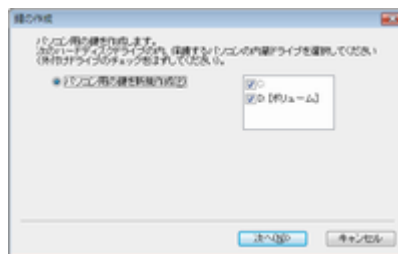
4.1　メディア鍵認証方式の場合

1. 再起動後に、以下の画面が表示されます。「OK」をクリックしてください。

Notice

「キャンセル」をクリックすると、本プログラムが終了します。その場合は、後で必ずスタートメニューから［すべてのプログラム］－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーティリティ］をクリックし、パソコンの鍵を作成および暗号化を行ってください。

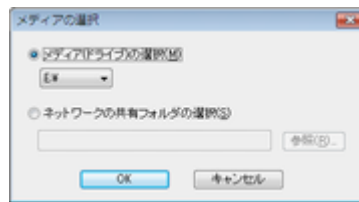
2. スーパーバイザパスワード入力画面が表示されます。
インストール時に設定したスーパーバイザパスワードを入力し、「OK」をクリックしてください。

3. 設定のご案内が表示されます。「次へ」をクリックしてください。

4. パソコンの鍵の作成に関する説明が表示されます。
内容を確認して準備ができたら、「次へ」をクリックしてください。

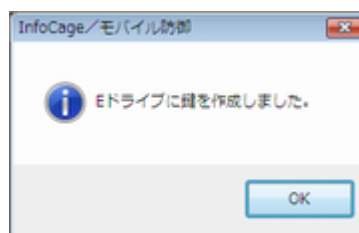
5. 「パソコン用の鍵を新規作成」が選択されています。ドライブ一覧に、内蔵ハードディスクドライブ以外のドライブが表示されている場合はチェックをはずしてください。
鍵を作成するメディアを装着し、「次へ」をクリックしてください。

Notice

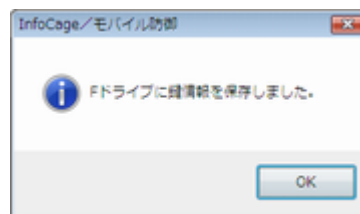
- システムドライブのチェックは外せません。
- 内蔵ハードディスクドライブは必ずチェックしてください。
内蔵ハードディスクドライブのチェックを外すと、その内蔵ハードディスクドライブへのデータのコピー、移動およびファイルの新規作成ができなくなったり、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しなくなったりする場合があります。
- 内蔵ハードディスクドライブではないドライブのチェックは必ずはずしてください。
内蔵ハードディスクドライブではないドライブにチェックをつけると、そのドライブを取り外した際に動作が不正になる場合があります。

6. 「鍵を格納するメディアまたは共有フォルダ」の「選択」をクリックしてください。

7. 「メディア（ドライブ）の選択」をクリックして選択し、ドライブ一覧から鍵を作成するメディアのドライブを選択してください。（ここでは例として E ドライブとします）

8. 「次へ」をクリックしてください。

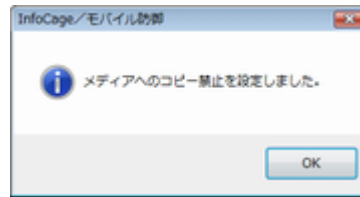
9. 内容を確認後、「作成」をクリックしてください。

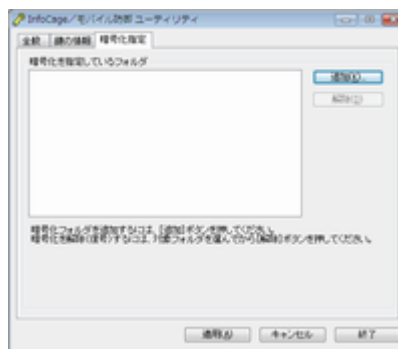
10. 鍵の作成が完了しました。「OK」をクリックしてください。

11. 続いて鍵情報を保存します。
鍵情報を保存するメディアを装着してください。
（ここでは例として F ドライブに保存します）
リムーバブルメディア（ドライブ）一覧に鍵情報を保存するメディアが見つからない場合は、「更新」をクリックしてください。
鍵情報の保存先メディアを選択し、「次へ」をクリックしてください。

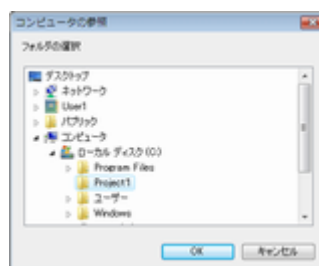
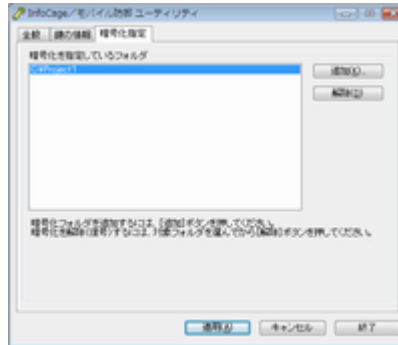
12. 鍵情報の保存が完了しました。「OK」をクリックしてください。

13. パソコンの保護に関する設定画面が表示されます。
データの抜き取り防止設定をする場合は、「メディアへのコピーを禁止する」のチェックを入れて「次へ」をクリックしてください。

Notice

- InfoCage モバイル防御の管理者の設定により外部メディア自動暗号が有効になっている場合、「メディアへのコピーを禁止する」は操作できません。
- 外部メディア自動暗号が無効になっている場合、ここにチェックをするとすべてのリムーバブルメディアへのデータのコピーができなくなります。

14. *13* で「メディアへのコピーを禁止する」のチェックを入れた場合、下記の画面が表示されます。
「OK」をクリックしてください。

15. 暗号化指定に関する説明が表示されます。
内容を確認して準備ができたら、「次へ」をクリックしてください。

16. 「暗号化指定」タブが表示されます。「追加」をクリックしてください。

Notice
InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが「暗号化を指定しているフォルダ」に表示されています。

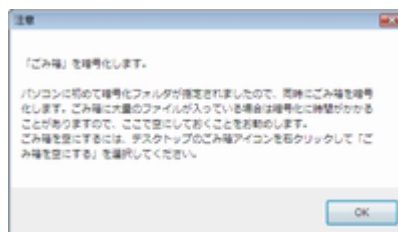
17. 暗号化したいドライブまたはフォルダを選択し、「OK」をクリックしてください。

18. 「暗号化を指定しているフォルダ」に選択したフォルダが追加されます。
複数のフォルダを指定したい場合は、*16* ～ *17* を繰り返してください。
暗号化したいドライブおよびフォルダを解除する場合は、「解除」をクリックしてください。
すべて指定し終わったら「適用」をクリックしてください。

Notice

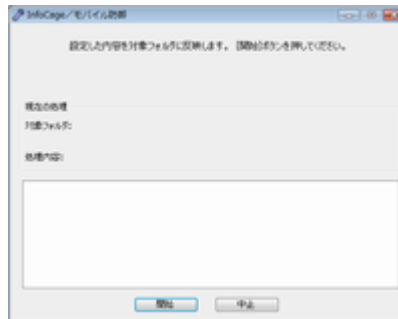
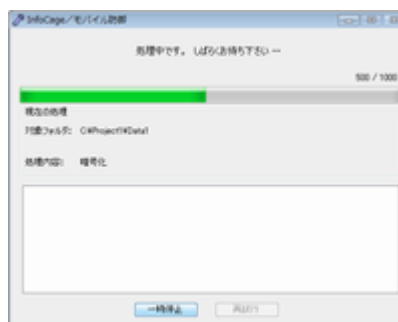
- すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、それらを「解除」後、「適用」または「終了」を実行するとそれらのフォルダは復号されますのでご注意ください。
- 「適用」をクリックすると、暗号化処理が終了するまで暗号化指定しているドライブおよびフォルダにはアクセスできなくなります。(「一時停止」をクリックしても同様です)
- ここで「終了」をクリックすると、指定したドライブおよびフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

19. 暗号化処理に関する注意事項が表示されます。
常駐アプリケーションや起動しているアプリケーションがあれば必ず終了し、「はい」をクリックしてください。

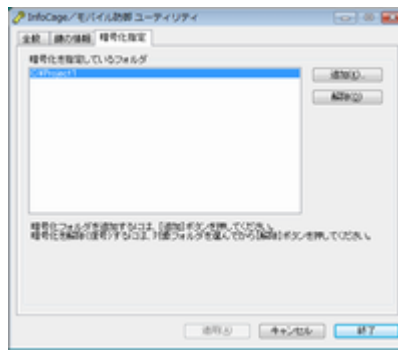
Notice

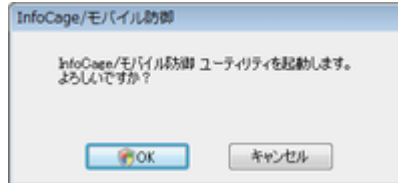
アプリケーションが使用しているファイルは、暗号化できない場合があります。

20. ごみ箱の暗号化に関する注意事項が表示されます。
ごみ箱に大量のファイルがある場合はごみ箱を空にしてから、「OK」をクリックしてください。

21. 「開始」をクリックすると、暗号化処理が始まります。

> **Notice**
>
> 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

22. 暗号化処理中です。しばらくお待ちください。

23. 暗号化処理が終了しました。
暗号化できなかったファイルがある場合はウィンドウ内に表示されます。
「終了」をクリックしてください。

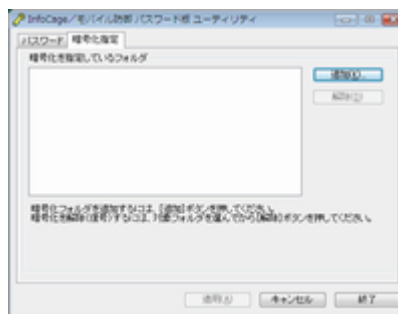
> **Notice**
>
> ・ 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、「再試行」をクリックしてください。
> すべての起動中のアプリケーションを終了して「再試行」をクリックしても暗号化できなかったファイルがある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗号化できません。これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録されるため、暗号化対象フォルダ内にあっても、動作に問題はありません。
>
> ・ 暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
>
> ・ 暗号化対象外ファイルについては、「InfoCage モバイル防御 ユーザーズガイド」の「「暗号化指定」タブ 」の項を参照してください。

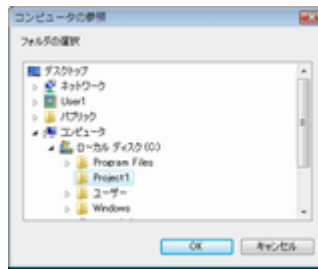
24.「暗号化を指定しているフォルダ」に暗号化されたフォルダが表示されます。
これで暗号化の作業は終了です。「終了」をクリックしてください。

その他の設定に関しては、「InfoCage　モバイル防御　ユーザーズガイド」を参照してください。

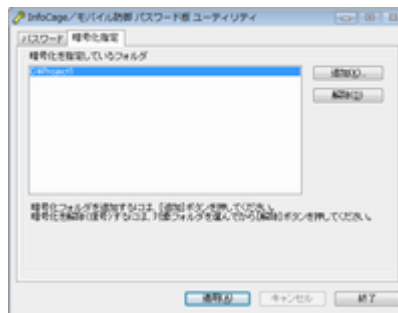
4.2　パスワード認証方式の場合

1. 再起動後に、以下の画面が表示されます。「OK」をクリックしてください。

> **Notice**
>
> 「キャンセル」をクリックすると、本プログラムが終了します。その場合は、後で必ずスタートメニューから［すべてのプログラム］－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーティリティ］をクリックし、暗号化を行ってください。

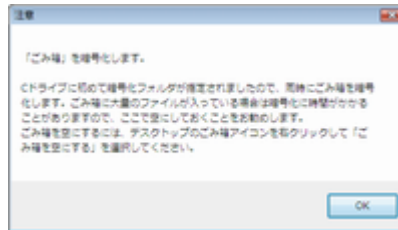
2. 初回起動時、Windows にログオンすると、自動で InfoCage モバイル防御ユーティリティが起動します。暗号化処理に関する説明が表示されますので、必ず内容を確認し、「OK」をクリックしてください。

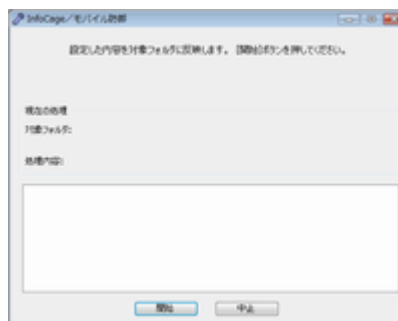
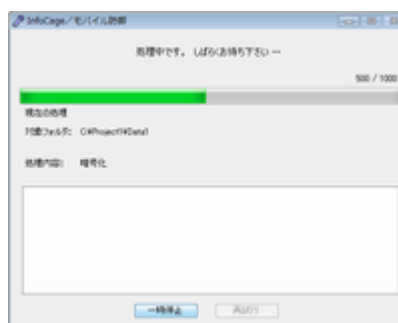
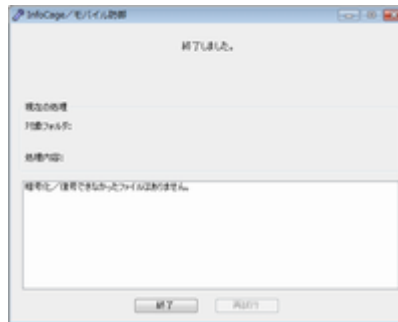
3. 「暗号化指定」タブが表示されます。「追加」をクリックしてください。

> **Notice**
>
> ・ InfoCage モバイル防御の管理者の設定により外部メディア自動暗号機能が有効の場合、システムドライブを除く暗号化フォルダの指定がない内蔵ハードディスクドライブは、リムーバブルメディアと同じ扱いとなり、その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなります。また、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しない場合がありますので、すべての内蔵ハードディスクドライブに暗号化フォルダを作成してください。

4. 暗号化したいドライブまたはフォルダを選択し、「OK」をクリックしてください。

5. 「暗号化を指定しているフォルダ」に選択したフォルダが追加されます。
複数のフォルダを指定したい場合は、 *3* ～*4* を繰り返してください。
暗号化したいドライブおよびフォルダを解除する場合は、「解除」をクリックしてください。
すべて指定し終わったら「適用」をクリックしてください。

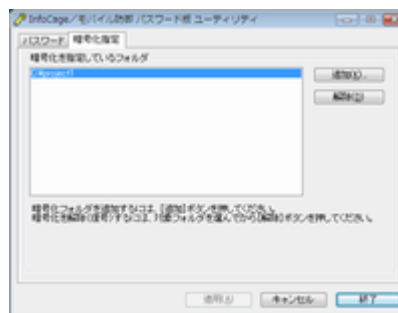
> **Notice**
>
> ・ すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、それらを「解除」後、「適用」または「終了」を実行するとそれらのフォルダは復号されますのでご注意ください。
>
> ・ 「適用」をクリックすると、暗号化処理が終了するまで暗号化指定しているフォルダにはアクセスできなくなります。（暗号化処理を実行中に「一時停止」をクリックしても同様です）
>
> ・ ここで「終了」をクリックすると、指定したフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

6. 暗号化処理に関する注意事項が表示されます。
常駐アプリケーションや起動しているアプリケーションがあれば必ず終了し、「はい」をクリックしてください。

> **Notice**
>
> アプリケーションが使用しているファイルは、暗号化できない場合があります。

7. ごみ箱の暗号化に関する注意事項が表示されます。
ごみ箱に大量のファイルがある場合はごみ箱を空にしてから、「OK」をクリックしてください。

8. 「開始」をクリックすると、暗号化処理が始まります。

> ⚠ **Notice**
> 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

9. 暗号化処理中です。しばらくお待ちください。

10. 暗号化処理が終了しました。
暗号化できなかったファイルがある場合はウィンドウ内に表示されます。
「終了」をクリックしてください。

⚠Notice

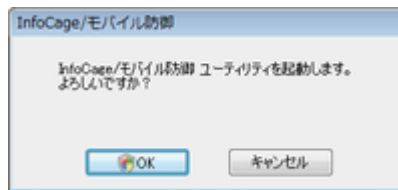
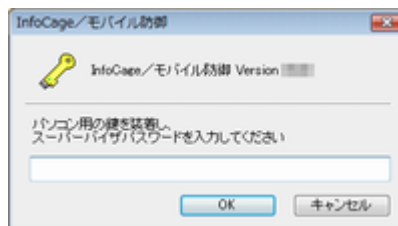
- 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、「再試行」をクリックしてください。
  すべての起動中のアプリケーションを終了して「再試行」をクリックしても暗号化できなかったファイルがある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗号化できません。これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録されるため、暗号化対象フォルダ内にあっても、問題はありません。
- 暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
- 暗号化対象外ファイルについては、「InfoCage モバイル防御 ユーザーズガイド」の「「暗号化指定」タブ 」の項を参照してください。

11. 暗号化を指定しているフォルダ」に暗号化されたフォルダが表示されます。
これで暗号化の作業は終了です。「終了」をクリックしてください。

その他の設定に関しては、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

第5章　ユーティリティの起動方法

InfoCage　モバイル防御　ユーティリティの起動方法を説明します。

1. スタートメニューから、［すべてのプログラム］－[NEC]－[InfoCage　モバイル防御]－[InfoCage　モバイル防御　ユーティリティ］をクリックします。

2. 「OK」をクリックしてください。

3. メディア鍵認証方式の場合は、鍵をパソコンに装着してからスーパーバイザパスワードを入力し、「OK」をクリックしてください。
パスワード認証方式の場合は、ユーザパスワードを入力し、「OK」をクリックしてください。
InfoCage　モバイル防御ユーティリティが起動します。

Notice
上記の画面はメディア鍵認証方式のものです。パスワード認証方式の場合は一部異なります。

● **InfoCage　モバイル防御　ユーザーズガイドを参照するには**

スタートメニューから、［すべてのプログラム］－[NEC]－[InfoCage　モバイル防御]－[InfoCage　モバイル防御　ユーザーズガイド］をクリックしてください。